PRIVACY GUIDE

February 2021 | 3725-49159-002A

Poly OBi Edition

Getting Help
For more information about installing, configuring, and administering Poly/Polycom products or services, go to Polycom Support.

Plantronics, Inc. (Poly — formerly Plantronics and Polycom)
345 Encinal Street
Santa Cruz, California
95060

Contents

Before You Begin

Topics:

The *Poly OBi Edition Privacy Guide* provides information regarding the implementation of Privacy by Design for this product.

This guide contains details about configurable privacy options and how personal data is processed. It covers the following Poly hardware:

- Poly VVX OBi Edition Business IP Phones
- Poly VVX D230 DECT IP Phones
- Poly OBi3 Series Voice Adapters
- Poly OBi5 Series Voice Adapters

Related Poly and Partner Resources

See the following sites for information related to this product.

- The Poly Online Support Center is the entry point to online product, service, and solution support information including Video Tutorials, Documents & Software, Knowledge Base, Community Discussions, Poly University, and additional services.
- The Polycom Document Library provides support documentation for active products, services, and solutions. The documentation displays in responsive HTML5 format so that you can easily access and view installation, configuration, or administration content from any online device.
- The Poly Community provides access to the latest developer and support information. Create an account to access Poly support personnel and participate in developer and support forums. You can find the latest information on hardware, software, and partner solutions topics, share ideas, and solve problems with your colleagues.
- The Poly Partners are industry leaders who natively integrate the Poly standards-based RealPresence Platform with their customers' current UC infrastructures, making it easy for you to communicate face-to-face with the applications and devices you use every day.
- The Poly Services help your business succeed and get the most out of your investment through the benefits of collaboration.

Privacy-Related Options

Topics:

There are different deployment options for your phone that may affect the privacy options and support requirements described in this guide. These details apply specifically to phones deployed on-premises in a customer environment and managed by the customer.

Passwords

You can change the administrator and user passwords.

Poly recommends that you change the default password at the earliest convenience.

Change the Default Password

If you use the default password, a warning message `Default password is used` appears at the top right of the page.

Change this password and record it in a safe place. If you lose this password, you may need to return your phone for service.

Procedure

1. In the system web interface, go to **System Management** > **Device Admin** > **Web Server**.
2. In the **Value** column, configure the following parameters:

Parameter	Description
`AdminPassword`	Enter a new, case- sensitive administrator password.
`AdminPin`	Enter a new, case- sensitive PIN to enter the updater menu.
`UserPassword`	Enter a new, case- sensitive user password.

3. Select **Submit**.
4. Reboot your system when you complete your changes.

Setting Up a Directory

Your phone supports a directory search function with an external server using LDAP. To use this function, you must configure an LDAP service on the phone.

You can point to the **Network Directory** option on the main menu of the phone to an LDAP service using LDAP parameters.

Configure the LDAP Server

Configure the LDAP server using the following parameters.

Procedure

1. In the system web interface, go to **IP Phone** > **LDAP** > **Server**.
2. In the **Value** column, configure the following parameters:

Parameter	Description
`Host`	Enter the hostname, which can be an IP address or domain name, with an optional `ldap://` or `ldaps://` scheme prefix. For example, `192.168.15.186, ldap.forums.com` or `ldap://ldap.testathon.net` are acceptable hostname formats. **Note:** If you don't specify the scheme, the phone uses `ldap://`.
`Port`	Enter the LDAP server listening (TCP) port. The standard port is 389 for `ldap://` and 636 for `ldaps://`. **Note:** If the port value is `0` or blank, the phone uses the corresponding standard port.
`Password`	Enter the bind password for simple or SASL authentication. **Note:** This parameter is case-sensitive.
`TLSSecurityProfile`	Enter the security profile for 802.1X authentication.

3. Select **Submit**.
4. Reboot your system when you complete your changes.

Configure LDAP SASL Authentication

Simple Authentication and Security Layer (SASL) involves sending the LDAP server the FQDN of the client and the corresponding password in clear-text.

This method has security issues unless you use `ldaps://` or TLS.

Note: LDAP v2 supports `ldap://` and `ldaps://` with simple authentication only. LDAP v3 adds support for TLS and SASL authentication.

For more information on SASL, go to http://www.openldap.org.

Procedure

1. In the system web interface, go to **IP Phone** > **LDAP** > **LDAP SASL Authentication Parameters**.
2. In the **Value** column, configure the following parameters:

Parameter	Description
`SASL_AuthMethod`	Select the method to use for SASL authentication using any of the following parameters: • Disabled (Default) • Plain • MD5
`SASL_AuthCID`	Enter the authentication ID for SASL authentication. The format of this ID depends on the actual SASL mechanism used.

3. Select **Submit**.
4. Reboot your system when you complete your changes.

Configure Speed Dial Keys

You can configure one or more feature keys as speed dials keys by assigning the `Function` parameter.

Procedure

1. In the system web interface, do one of the following:
   - Go to **IP Phone** > ***n*** **Line Keys** (where *n* = Left or Right).
   - Go to **IP Phone** > **Programmable Keys**.
2. Select a key (for example, **Key 1** or **Key 2**).
3. In the **Default** column for the `Function`, clear the check box.
4. In the **Value** column for the `Function` parameter, select **Speed Dial**.
5. Select **Submit**.
6. Reboot your system when you complete your changes.

Saving and Erasing Call History

The **Call History** page shows the last 200 calls.

You can view the following detailed call information:

- The terminals involved
- The name (if available) of the peer endpoints making the call
- The direction/path the call took
- The time events took place

Save the Call History

You can save the phone's call history from the system web interface.

Procedure

1. In the system web interface, go to **Status** > **Call History**.
2. Select **Save All**.

   The phone saves the call history to the `callhistory.xml` file in your `Downloads` folder.

Erase the Call History

You can erase the phone's call history from the web interface.

Procedure

1. In the system web interface, go to **Status** > **Call History**.
2. Select **Remove All**.

   The phone permanently erases the call history.

SIP Privacy

Your phone observes inbound caller privacy and decodes the caller's name and number from SIP `INVITE` requests by checking the `FROM`, P-Asserted-Identity (`PAID` for short), and Remote-Party-ID (`RPID` for short) message headers.

All these headers can carry caller's name and number information.

Enable an RPID Header

For outbound calls, the phone can state the caller's preferred privacy setting in an `RPID` header of the outbound `INVITE` request.

Procedure

1. In the system web interface, go to **Service Providers** > **ITSP Profile *X*** > **SIP** (where *X*=the ITSP profile for the service provider).
2. In the **Value** column for the `X_InsertRemotePartyID` parameter, select the check box (the default value of this parameter).
3. Select **Submit**.
4. Reboot your system when you complete your changes.

Block Outbound Caller ID

You can instruct your phone to use `sip:anonymous@localhost` in the `FROM` header to block outbound caller ID.

Procedure

1. In the system web interface, go to **Service Providers** > **ITSP Profile *X*** > **SIP** (where *X*=the ITSP profile for the service provider).

2. In the **Value** column for the `X_UseAnonymousFROM` parameter, select the check box.

   Your phone also includes a `Privacy: id` header if the `X_InsertPrivacyHdr` parameter is enabled.
3. Select **Submit**.
4. Reboot your system when you complete your changes.

Logs

Logs contain information about system activities and configurations to help you troubleshoot issues.

Enable Network Call Logs

The network call logs consist of four logs: All, Missed, Received, and Outgoing.

The server stores log data and downloads it to the phone when you invoke this function. Consult BroadSoft on how to manage these call logs on the server side.

To make the network call logs function available on the phone, you must enable the option `CallLogs` parameter. There's no specialized app, feature key function, or softkey option to launch network call logs. You can only invoke this function by going through the Net Services app.

If you enable the Buddy List and it's available under the same SP service, the phone displays the presence icon in the network directory.

Procedure

1. In the system web interface, go to **Voice Services** > **SPn Service** > **Network Provided Services**.
2. In the **Value** column for the `CallLogs` parameter, select the check box.
3. Select **Submit**.
4. Reboot your system when you complete your changes.

Factory Resetting Your Phone

You can reset all configuration parameters to factory default values or to the customized default values.

Factory Reset Your Phone in the Local Interface

You can reset all phone settings to factory default values from the phone's local interface.

Procedure

1. Go to **Settings**.
2. Press the **Factory Reset** softkey.
3. Press the **OK** softkey.

Factory Reset Your Phone in the System Web Interface

You can reset the phone user data and voice configuration settings to factory default values in the system web interface.

Procedure

1. In the system web interface, go to **System Management** > **Device Update** > **Reset Configuration**.
2. Select **User Data**, **Voice Configuration**, **Networking**, or all three.
3. Select **Reset**.

How Data Subject Rights Are Supported

Topics:

The following information shows how data subject rights are supported.

Right to Access

View system details

Information pertaining to the device such as device IP address, serial number, and MAC address are shown on the system web interface and device local interface. An administrator can check them on web page or on the device local interface (under the **Product Information** menu). A user can access the call logs and phone book on the device local interface.

Note: Password information isn't revealed in the system web interface or the device local interface.

Procedure:

1. Connect the phone to the network.
2. From the device local interface, go to the **Product Information** menu and note the IP address of the phone.
3. From a web browser, go to the IP address of the phone and log in as admin.
4. Click the link on the left side panel to view the corresponding pages.

A copy of any personal data made available to Polycom when working with Polycom support is available by requesting it from your Polycom support representative.

Right To Be Informed

What personal data is collected?

See Purposes for Processing Personal Data on page 13.

How is personal data used?

See Purposes for Processing Personal Data on page 13.

How long is personal data kept?

Customer personal data is kept until a factory reset is performed. See How Personal Data is Deleted. In addition, a user can remove the personal phone book and user-level call logs directly from the device local interface without needing factory reset.

Any personal data made available when working with Polycom support, specific to a support incident, is retained until the information is requested to be removed by the customer.

Is personal data shared with any third parties and if so, who?

If personal data is made available when working with Polycom support, this data may be shared with Polycom's engineering team (which may include third parties / contractors).

How can a data subject be notified of a data breach?

Data subjects have a right to be notified when their data has been processed without authorization. The product administrator is able to monitor and identify when certain security anomalies have occurred. See How Administrators Are Informed of Any Security Anomalies on page 14.

Right to Data Portability

Subject to approval by the device admin, the user may obtain a backup copy of all the web pages in XML file format.

These backup pages can be viewed directly as text files or restored into a similar device to be viewed as web pages. Similarly, the user can get a copy of the personal phone book and user-level call logs by uploading each to a server in an XML format. A backup copy of the system-level call history can be obtained from the system web interface with help from the device admin. Note that all password fields are excluded from backup copies of the web pages.

Right to Erasure

A data subject has the right to remove all his or her own personal data. For details on how to erase customer personal data from the system, see How Personal Data is Deleted on page 16.

Any personal data made available when working with Polycom support, specific to a support incident, is retained until the information is requested to be removed by the customer.

Right to Rectification

A data subject has the right to make corrections to their own inaccurate or incomplete personal data. Personal data specific to device configuration can be edited or updated by the device administrator. See Privacy-Related Options on page 4.

Polycom does not manipulate data made available during the support process, so any rectification of inaccuracies of personal data must be performed by customer directly.

Right to Object to Processing

Not applicable because the customer is the controller.

Right to Restrict Processing

Not applicable because the customer is the controller.

Purposes for Processing Personal Data

Purposes for Processing Personal Data

Personal Data Category	Type of Personal Data	Purpose of Processing	Interface Type
Call Logs	▪ Peer Caller ID Name and Number ▪ Timestamp ▪ Call Duration ▪ Call Statistics (such as MOS score)	Provide call history with call statistics for each call	▪ System web interface for system level call logs ▪ Local interface for user level call logs
Personal Phone Book	Contact information: ▪ Name ▪ Number	Allow user to make calls from the phone book	Local interface
SYSLOG	The detail types of data to include are configurable. Typically, it includes: ▪ Boot up/system initialization information ▪ Network initialization information ▪ Call events ▪ Network/system events It can include SIP Transactions for REGISTER, SUBSCRIBE/NOTIFY, and Call Signaling for all calls on certain lines. **Note:** The phone does not store syslog files internally. It only sends the log to the configured syslog server to be stored and processed.	Troubleshooting	System web interface
PCAP	All network traffic	Troubleshooting	System web interface

How Administrators Are Informed of Any Security Anomalies

How Administrators are Informed of Any Security Anomalies (Including Data Breaches)

Security Anomaly Type	Where to Check	Recommended Frequency to Check
System reboots and crashes	▪ Device LED and local interface indicate clearly if the device has rebooted. ▪ Reboot events are recorded in SYSLOG logs that indicate the reason for each reboot (or no reason if the system crashes).	Check the log file after each reboot to analyze the reason for the reboot.

Log Type

Log Type	Description	Purpose	Location
SYSLOG	The detail types of data to include are configurable. Typically, it includes: ▪ Boot up/system initialization information ▪ Network initialization information ▪ Call events ▪ Network/system events It can include SIP Transactions for REGISTER, SUBSCRIBE/NOTIFY, and Call Signaling for all calls on certain lines. **Note:** The phone does not store syslog files internally. It only sends the log to the configured syslog server to be stored and processed.	Troubleshooting	System web interface
PCAP	All network traffic	Troubleshooting	System web interface

How Personal Data is Deleted

How Personal Data is Deleted

Data Type	Steps to Delete	Deletion Method
Credentials: ▪ SIP ▪ Web ▪ Network ▪ Wi-Fi	Factory Reset via system web interface: **1.** Go to the **Device Management/Device Update** web page. **2.** Check **Voice Configuration**. **3.** Select **Reset**.	Internal configuration file removal with disk overwritten.
User-Level Call Logs	From the local interface: **1.** Go to **Main Menu/Call History**. **2.** Select **Clear List**. From the system web interface: **1.** Go to the **Device Management/Device Update** page. **2.** Check the **User Data** option. **3.** Select **Reset**. **Note:** This method also removes system-level call logs and personal phone book.	Internal call history file removal with disk overwritten.
System-Level Call Logs	From the system web interface: **1.** Go to the **Device Management/Device Update** page. **2.** Check the **User Data** option. **3.** Select **Reset**. **Note:** This method also removes user-level call logs and personal phone book.	Internal call history file removal with disk overwritten.

Data Type	Steps to Delete	Deletion Method
Phone Book	From the local interface: 1. Go to **Main Menu/Contacts**. 2. Select **Remove All**. From the system web interface: 1. Go to the **Device Management/Device Update** page. 2. Check the **User Data** option. 3. Select **Reset**. **Note:** This method also removes system-level and user-level call logs.	Internal phone book file removal with disk overwritten.